

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

01/4/2011

SUBJECT:

Vulnerability in Windows Graphics Rendering Engine Could Allow Remote Code Execution

OVERVIEW: A new vulnerability has been discovered in Microsoft Windows Graphics Rendering Engine, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user views a specially crafted thumbnail image. In an email or web-based attack scenario, exploitation may occur if a user opens or previews a document containing a specially crafted thumbnail image received as an email attachment or hosted on a website. Alternatively, an attacker can place the specially crafted thumbnail image on a network share and convince the user to navigate to the file location using Windows Explorer. Successful exploitation of the vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is currently no patch available for this vulnerability and a working Metasploit Framework exploit module is available which results in remote code execution. The exploit has been tested by the MS-ISAC against a fully patched Windows XP SP3 system and confirmed to result in remote code execution.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008 SP2 and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
 - Small business entities: **High**
- Home users: **High**

DESCRIPTION:

A new vulnerability has been discovered in Microsoft Windows Graphics Rendering Engine, which could allow an attacker to take complete control of an affected system. The vulnerability occurs when the Graphics Rendering Engine component of the operating system improperly parses a specially crafted thumbnail image. This may result

in a stack overflow condition, allowing the attacker to execute arbitrary code in the context of the logged-on user.

In an email or web-based attack scenario, exploitation may occur if a user opens or previews a document containing a specially crafted thumbnail image received as an email attachment or hosted on a website. Alternatively, an attacker can place the specially crafted thumbnail image on a network share and convince the user to navigate to the file location using Windows Explorer. Successful exploitation of the vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Until a patch is available, Microsoft has posted details of a workaround in their advisory (see references below). The workaround lists how to modify the access control list (ACL) on *shimgvw.dll*. Please note that while this workaround will prevent the vulnerability being from exploited on vulnerable systems, media files typically handled by the Graphics Rendering Engine will not be displayed properly.

It should be noted that there is currently no patch available for this vulnerability and a working Metasploit Framework exploit module is available which results in remote code execution. The exploit has been tested by the MS-ISAC against a fully patched Windows XP SP3 system and confirmed to result in remote code execution.

RECOMMENDATIONS:

The following actions should be taken:

- After analyzing the business impact, consider implementing the ACL workaround provided by Microsoft (see [Microsoft Advisory 2490606](#)).
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Remind users not to download or open files from untrusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/2490606.mspx>

SANS:

<http://isc.sans.edu/diary.html?storyid=10201>

SecurityFocus:

<http://www.securityfocus.com/bid/45662>

Threatpost:

https://www.metasploit.com/redmine/projects/framework/repository/revisions/11466/entry/modules/exploits/windows/fileformat/ms11_xxx_createsizeddibsection.rbhttp://threatpost.com/en_us/blogs/microsoft-warns-security-hole-windows-graphics-engine-010411

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3970>